Yee & Associates, P.C.

4100 Alpha Road
Suite 1100
Dallas, Texas 75244

Main No. (972) 385-8777
Facsimile (972) 385-7766

Facsimile Cover Sheet

To: Commissioner for Patents for **Examiner Matthew T. Henning Group Art Unit 2131**	Facsimile No.: **703/872-9306**
From: Michele Morrow for Jane Roberts Legal Assistant to James O. Skarsten	No. of Pages Including Cover Sheet: **32**

Message:

Enclosed herewith:

- Transmittal Document; and
- Appeal Brief.

Re: Application No. **09/740,400**
Attorney Docket No: **AUS920000798US1**

Date: Tuesday, May 24, 2005

Please contact us at (972) 385-8777 if you do not receive all pages indicated above or experience any difficulty in receiving this facsimile.

PLEASE CONFIRM RECEIPT OF THIS TRANSMISSION BY FAXING A CONFIRMATION TO 972-385-7766.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: **Bones et al.**

Serial No.: **09/740,400**

Filed: **December 18, 2000**

For: **Incorporating Password Change Policy Into a Single Sign-On Environment**

35525
PATENT TRADEMARK OFFICE
CUSTOMER NUMBER

§ Group Art Unit: **2131**
§
§ Examiner: **Henning, Matthew T.**
§
§ Attorney Docket No.: **AUS920000798US1**
§
§
§
§

Certificate of Transmission Under 37 C.F.R. § 1.8(a)
I hereby certify this correspondence is being transmitted via facsimile to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, facsimile number (703) 872-9306 on May 24, 2005.

By: Michele Morrow
Michele Morrow

TRANSMITTAL DOCUMENT

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:
ENCLOSED HEREWITH:

- Appeal Brief (37 C.F.R. 41.37).

A fee of $500.00 is required for filing an Appeal Brief. Please charge this fee to IBM Corporation Deposit Account No. 09-0447. No additional fees are believed to be necessary. If, however, any additional fees are required, I authorize the Commissioner to charge these fees which may be required to IBM Corporation Deposit Account No. 09-0447. No extension of time is believed to be necessary. If, however, an extension of time is required, the extension is requested, and I authorize the Commissioner to charge any fees for this extension to IBM Corporation Deposit Account No. 09-0447.

Respectfully submitted,

James O. Skarsten

James O. Skarsten
Registration No. 28,346
Duke W. Yee
Registration No. 34,285
YEE & ASSOCIATES, P.C.
P.O. Box 802333
Dallas, Texas 75380
(972) 385-8777
ATTORNEYS FOR APPLICANTS

RECEIVED
CENTRAL FAX CENTER
MAY 24 2005

Docket No. AUS920000798US1 *PATENT*

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: **Bones et al.**	§	
	§	Group Art Unit: **2131**
Serial No. **09/740,400**	§	
	§	Examiner: **Henning, Matthew T.**
Filed: **December 18, 2000**	§	
	§	
For: **Incorporating Password Change Policy Into a Single Sign-On Environment**	§	

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Certificate of Transmission Under 37 C.F.R. § 1.8(a)
I hereby certify this correspondence is being transmitted via facsimile to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, facsimile number (703) 872-9306 on May 24, 2005.

By: Michele Morrow
Michele Morrow

APPEAL BRIEF (37 C.F.R. 41.37)

This brief is in furtherance of the Notice of Appeal, filed in this case on March 24, 2005.

The fees required under § 41.20(B)(2), and any required petition for extension of time for filing this brief and fees therefore, are dealt with in the accompanying TRANSMITTAL OF APPEAL BRIEF.

05/26/2005 EFLORES 00000098 090447 09740400
01 FC:1402 500.00 DA

REAL PARTY IN INTEREST

The real party in interest in this appeal is the following party: International Business Machines Corporation.

RELATED APPEALS AND INTERFERENCES

With respect to other appeals or interferences that will directly affect, or be directly affected by, or have a bearing on the Board's decision in the pending appeal, there are no such appeals or interferences.

STATUS OF CLAIMS

A. TOTAL NUMBER OF CLAIMS IN APPLICATION

Claims in the application are: 1-57

B. STATUS OF ALL THE CLAIMS IN APPLICATION

1. Claims canceled: NONE
2. Claims withdrawn from consideration but not canceled: NONE
3. Claims pending: 1-57
4. Claims allowed: NONE
5. Claims rejected: 1-57
6. Claims objected to: NONE

C. CLAIMS ON APPEAL

The claims on appeal are: 1-57

STATUS OF AMENDMENTS

A Response to Final Office Action was filed on January 26, 2005, however, no claims were amended in the Response. Therefore, the claims on Appeal herein are as originally filed and as finally rejected in the Final Office Action dated November 24, 2004.

SUMMARY OF CLAIMED SUBJECT MATTER

A. CLAIM 1 - INDEPENDENT

The subject matter of claim 1 is directed to a method, in a data processing system, for changing a plurality of target passwords in a single sign-on environment. In response to receiving a change instruction identifying a first single sign-on password, the first single sign-on password is changed to create a second single sign-on password (page 16, lines 22-27; Steps **502-506** in **Figure 5**). A target password is retrieved (page 16, lines 27-28; Step **508** in **Figure 5**), and the target password is modified in a user selected manner to match the second single sign-on password to create a modified target password (page 17, lines 7-11; Step **516**; page 17, line 19-page 18, line 13; **Figure 6**).

B. CLAIM 20 – INDEPENDENT

The subject matter of claim 20 is directed to a computer program product in computer readable media for use in a data processing system for changing a plurality of target passwords in a single sign-on environment. The computer program product has first instructions for, in response to receiving a change instruction identifying a first single sign-on password, changing the first single sign-on password to create a second single sign-on password (page 16, lines 22-27; Steps **502-506** in **Figure 5**). The computer program product further has second instructions for retrieving a target password (page 16, lines 27-28; Step **508** in **Figure 5**), and third instructions for modifying the target password in a user selected manner to match the second single sign-on password to create a modified target password (page 17, lines 7-11; Step **516**; page 17, line 19-page 18, line 13; **Figure 6**).

C. CLAIM 39 - INDEPENDENT

The subject matter of claim 39 is directed to a system for changing a target password in a single sign-on environment. The system includes, in response to receiving a change instruction

identifying a first single sign-on password, means for changing the first single sign-on password to create a second single sign-on password (page 10, line 1 to page 11, line 17; data processing system **300** in **Figure 3**; also see page 16, lines 22-27; Steps **502-506** in **Figure 5**). The system also includes a means for retrieving a target password (page 10, line 1 to page 11, line 17; data processing system **300** in **Figure 3**; also see page 16, lines 27-28; Step **508** in **Figure 5**), and means for modifying the target password in a user selected manner to match the second single sign-on password to create a modified target password (page 10, line 1 to page 11, line 17; data processing system **300** in **Figure 3**; also see page 17, lines 7-11; Step **516**; page 17, line 19-page 18, line 13; **Figure 6**).

D. CLAIM 16 – DEPENDENT

The subject matter of claim 16, which depends from claim 1, is directed to a method in a data processing system for changing a plurality of target passwords in a single sign-on environment, wherein, responsive to a determination that a target password has been retrieved (page 18, lines 20-21; Step **702** in **Figure 7**), a change target password policy is determined, and the change target password policy is applied to modify the target password to match a second single sign-on password to create modified target password (page 18, lines 21-24; Steps **704** and **706** in **Figure 7**; and page 18, line 25 to page 24, line 5; **Figures 8** and **9**).

E. CLAIM 35 – DEPENDENT

The subject matter of claim 35, which depends from claim 20, is directed to a computer program product in computer readable media for use in a data processing system for changing a plurality of target passwords in a single sign-on environment, wherein the computer program product further includes fourth instructions for, responsive to a determination that a target password has been retrieved (page 18, lines 20-21; Step **702** in **Figure 7**), determining a change target password policy, and fifth instructions for, responsive to the fourth instructions, applying the

change target password policy to modify the target password to match a second single sign-on password to create a modified target password (page 18, lines 21-24; Steps **704** and **706** in **Figure 7**; and page 18, line 25 to page 24, line 5; **Figures 8** and **9**).

F. CLAIM 54 – DEPENDENT

The subject matter of claim 54, which depends from claim 39, is directed to a system for changing a target password in a single sign-on environment. The system further includes responsive to a determination that a target password has been retrieved (page 10, line 1 to page 11, line 17; data processing system **300** in **Figure 3**; also see page 18, lines 20-21; Step **702** in **Figure 7**), means for determining a change target password policy, and responsive to the means for determining a change target password policy, means for applying the change target password policy to modify the target password to match a second single sign-on password to create a modified target password (page 10, line 1 to page 11, line 17; data processing system **300** in **Figure 3**; also see page 18, lines 21-24; Steps **704** and **706** in **Figure 7**; and page 18, line 25 to page 24, line 5; **Figures 8** and **9**).

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

A. GROUND OF REJECTION 1 (Claims 1-14, 20-33, 39-52)

Claims 1-14, 20-33 and 39-52 stand rejected under 35 U.S.C. §102(b) as being anticipated by He (U.S. Patent No. 5,944,824).

B. GROUND OF REJECTION 2 (Claims 15, 34, 53)

Claims 15, 34 and 53 stand rejected under 35 U.S.C. §103(a) as being unpatentable over He in view of Redpath (U.S. Patent 5,854,629).

C. GROUND OF REJECTION 3 (Claims 16, 35, 54)

Claims 16, 35 and 54 stand rejected under 35 U.S.C. §103(a) as being unpatentable over He in view of Prafullchandra (U.S. Patent 5,734,718).

D. GROUND OF REJECTION 4 (Claims 17-19, 36-38, 55-57)

Claims 17-19, 36-38 and 55-57 stand rejected under 35 U.S.C. §103(a) as being unpatentable over He in view of Prafullchandra.

ARGUMENT

A. GROUND OF REJECTION 1 (Claims 1-14, 20-33, 39-52)

The Examiner has rejected claims 1-14, 20-33 and 39-52 under 35 U.S.C. §102(b) as being anticipated by He (U.S. Patent No. 5,944,824).

Claim 1 of the present application reads as follows:

> 1. A method in a data processing system for changing a plurality of target passwords in a single sign-on environment, comprising the steps of:
> in response to receiving a change instruction identifying a first single sign-on password, changing the first single sign-on password to create a second single sign-on password;
> retrieving a target password; and
> modifying the target password in a user selected manner to match the second single sign-on password to create a modified target password.

A prior art reference anticipates a claimed invention under 35 U.S.C. § 102 only if every element of the claimed invention is identically shown in that single prior art reference, arranged as they are in the claims. *In re Bond*, 910 F.2d 831, 832, 15 U.S.P.Q.2d 1566, 1567 (Fed. Cir. 1990). All limitations of a claimed invention must be considered when determining patentability. *In re Lowry*, 32 F.3d 1579, 1582, 32 U.S.P.Q.2d 1031, 1034 (Fed. Cir. 1994). Anticipation focuses on whether a claim reads on the product or process a prior art reference discloses, not on what the reference broadly teaches. *Kalman v. Kimberly-Clark Corp.*, 713 F.2d 760, 218 U.S.P.Q. 781 (Fed. Cir. 1983).

Appellants respectfully submit that He does not identically show every element of the claimed invention arranged as they are in the claims; and, accordingly, does not anticipate the claims. With respect to claim 1, in particular, Appellants submit that He does not disclose "in response to receiving a change instruction identifying a first single sign-on password, changing the first single sign-on password to create a second single sign-on password" and "modifying the target password in a user selected manner to match the second single sign-on password to create a modified target password" as recited in the claim.

In rejecting the claims, the Examiner states the following with respect to claim 1:

> Claim 1 recites changing the SSO password in response to receiving a change instruction. He disclosed a programmed method and system for changing passwords in a Single Sign-On (SSO) environment (See He Col. 13, Paragraph 3-7). He disclosed that in response to a request to modify a user account (See He Col. 13 Lines 12-13) a new password is generated (See He Col. 13 Lines 20-22) and the old password is set to the new password (See He Col. 13 Lines 43-45).
>
> Claim 1 further recites retrieving and modifying a target password. He disclosed changing a target NE password to the specified new password (See He Col. 13 Lines 31-35.

Final Office Action dated November 24, 2004, page 3.

He is directed to permitting a single sign-on (SSO) of users to a plurality of network elements, and describes data structures and procedures that support the SSO functionality in a distributed network environment. He does not relate to changing an SSO password, and does not disclose changing a first single sign-on password to a second single sign-on password in response to receiving a change instruction identifying the first single sign-on password.

Col. 13, Paragraphs 3-7 of He referred to by the Examiner as disclosing "in response to receiving a change instruction identifying a first single sign-on password, changing the first single sign-on password to create a second single sign-on password" reads as follows:

> Precondition **250**: A user account is being created or modified. Access by the user **12** to an NE **20** is defined and the user **12** is granted with the SSO capability to this NE **20**. The network security administrator **17** who is carrying out the task is an authenticated user to the security server **15** node.
>
> The <User Log-on Identifier> is created **252** randomly or manually for the user account. The <Present Password> is created **254** randomly or manually for the user account. The <New Password> is created **256** randomly or manually for the user account. Next, the NE record is fetched **258** from the security database **13** at the security server **15** node. The <Super-User Logon Identifier, Present Password, New Password> for the NE is retrieved **260** from the record.
>
> At this point, the process continues when a message containing <Super- User Log-on Identifier, Present Password, New Password> for the NE along with <NE, User Log-on Identifier, Present Password> for the user account is sent **262** to the secure terminal server **24** that serves the NE. The secure terminal server **24** invokes a local procedure **263** that performs the log-in sequence of the NE **20**, logs in as a super user, creates or resets the user account in the NE **20** changes the super user password to a new

one using the data provided in the message. The security server **15** returns control to the main procedure at the security server **15** node on successful completion of the steps.

Next, the <Present Password> for the super user is set **264** to the value of <New Password> in the same record and set the <New Password> for the super user **94** to a randomly generated one. This data is written **266** into the super user account in the security database **13** at the security server **15**. The process continues with the <NE User Log-on Identifier, Present Password, New Password> written **268** into the user account in the security database **13** at the security server **15**.

Post result **270**: The user password entry is created for the user account and is synchronized with that in the NE **20**.

Col. 13, Paragraphs 3-7 of He does not discuss changing an SSO password and certainly does not disclose the claimed step of "in response to receiving a change instruction identifying a first single sign-on password, changing the first single sign-on password to create a second single sign-on password". The paragraphs instead relate to the precondition that a user account is being created or modified, and that access to an NE (Network Element) is defined and granted to a user with SSO capability The paragraphs do not discuss changing an SSO password. The reference only discloses changing an NE password or a super user password which is not a single sign-on password. In particular, a "super user password" is specifically described in Col. 11 Lines 3-11 of He as follows:

> The "Super-User Log-On Identifier" **142** should be different from the one that is used by network security administrator **17** for interaction with the NE **20**. The existence of this separate super user identifier **142** supports the implementation of SSO. The super user **94** requires the privileges to create regular user accounts, to set up the initial user passwords, and to change user passwords in the NE **20**. This enhancement only affects the security server **15** node in the security database **13**. (Emphasis added.)

Thus, He clearly describes that the super user identifier is not a single sign-on password, but is a separate identifier that supports the implementation of a single sign-on password, and that provides a "super user" the privileges to create regular user accounts and the like. The Examiner, accordingly, is contradicting the clear disclosure in He by interpreting the super user password as being a single sign-on password.

He also does not disclose the claimed step of "modifying the target password in a user selected manner to match the second single sign-on password to create a modified target password". The Examiner refers to Col. 13, lines 31-35 of He as disclosing this feature. Col. 13,

lines 31-35, which is reproduced above, is again reproduced for the convenience of the Board:

> The secure terminal server **24** invokes a local procedure **263** that performs the log-in sequence of the NE **20**, logs in as a super user, creates or resets the user account in the NE **20** changes the super user password to a new one using the data provided in the message.

Although, as indicated above, He may disclose changing a super user password, the reference nowhere discloses changing a first SSO password to a second SSO password. Accordingly, He the also does not disclose "modifying the target password in a user selected manner to match the second single sign-on password to create a modified target password" as recited in claim 1. Only the present application contains such a disclosure.

In responding to arguments made by Appellants in the Response to Office Action filed August 16, 2004, the Examiner stated:

> 32. Regarding the argument that He does not disclose changing SSO passwords, He disclosed that at least one super user has SSO capability (See He Col. 8 Lines 47-49). If the super user was a SSO super user, then changing the passwords of the super user, as disclosed in col. 13 Paragraphs 3-7, must have involved changing SSO passwords, as specifically discussed below.

Final Office Action dated November 24, 2004, page 8.

The Examiner then specifically refers to col. 13, lines 27-28 of He as describing a first SSO password, and col. 13, lines 34-35 as disclosing changing the first SSO password to a new SSO password. Appellants respectfully disagree. He, in col. 13, lines 26-35 states:

> At this point, the process continues when a message containing <Super- User Log-on Identifier, Present Password, New Password> for the NE along with <NE, User Log-on Identifier, Present Password> for the user account is sent **262** to the secure terminal server **24** that serves the NE. The secure terminal server **24** invokes a local procedure **263** that performs the log-in sequence of the NE **20**, logs in as a super user, creates or resets the user account in the NE **20** changes the super user password to a new one using the data provided in the message.

The above recitation only discusses changing a super user password, and does not disclose or relate to changing an SSO password. As discussed above, Col. 13, Paragraphs 3-7 of He generally relate to the precondition that a user account is being created or modified, and that access to an NE (Network Element) is defined and granted to a user with SSO capability. The paragraphs do not disclose changing an SSO password, but only disclose changing an NE password or a super user password. He does not disclose "in response to receiving a change instruction identifying a first single sign-on password, changing the first single sign-on password to create a second single sign-on password" as recited in independent claim 1, and does not anticipate claim 1.

For at least all the above reasons, claim 1 is not anticipated by He, and claim 1 should be allowable over He in its present form.

Claims 2-14 depend from and further restrict claim 1, and are also not anticipated by He, at least by virtue of their dependency.

Independent claim 20 is a computer program product claim counterpart to method claim 1, and recites limitations similar to claim 1. Claim 20, accordingly, is also not anticipated by He for substantially the same reasons as discussed above with respect to claim 1.

Claims 21-33 depend from and further restrict independent claim 20, and are also not anticipated by He, at least by virtue of their dependency.

Independent claim 39 is system claim counterpart to method claim 1, and recites limitations similar to claim 1. Claim 39, accordingly, is also not anticipated by He for substantially the same reasons as discussed above with respect to claim 1.

Claims 40-52 depend from and further restrict independent claim 39, and are also not anticipated by He, at least by virtue of their dependency.

Therefore, claims 1-14, 20-33 and 39-52 are believed to patentably distinguish over He, and it is respectfully requested that the Board reverse the Examiner's final rejection of those claims.

B. GROUND OF REJECTION 2 (Claims 15, 34, 53)

Claims 15, 34 and 53 stand rejected under 35 U.S.C. §103(a) as being unpatentable over He in view of Redpath (U.S. Patent 5,854,629).

In rejecting claims 15, 34 and 53, the Examiner acknowledges that He does not disclose the use of a Graphical User Interface (GUI) for implementing selection of a password. The Examiner contends, however, that Redpath teaches that GUIs were created in order to simplify interaction with computer programs for end users of computer programs, and concludes that it would have been obvious to the ordinary person skilled in the art at the time of the invention to employ the teachings of Redpath in He such that the user is supplied a GUI menu in order to select a password generation method.

Claims 15, 34 and 53, however, depend from and further restrict independent claims 1, 20 and 39, respectively, and Redpath does not supply the deficiencies in He as discussed in detail above. Accordingly, for at least the reasons discussed above, claims 15, 34 and 53 are not obvious over He in view of Redpath.

Therefore, claims 15, 34 and 53 are believed to patentably distinguish over He in view of Redpath, and it is respectfully requested that the Board reverse the Examiner's final rejection of those claims.

C. GROUND OF REJECTION 3 (Claims 16, 35, 54)

Claims 16, 35 and 54 stand rejected under 35 U.S.C. §103(a) as being unpatentable over He in view of Prafullchandra (U.S. Patent 5,734,718).

Initially, claims 16, 35 and 54 depend from and further restrict independent claims 1, 20 and 39, respectively, and Prafullchandra does not supply the deficiencies in He as discussed in detail above. Accordingly, for at least the reasons discussed above, claims 16, 35 and 54 are not obvious over He in view of Prafullchandra.

In addition, Appellants respectfully submit that claims 16, 35 and 54 are independently patentable over He in view of Prafullchandra. Claim 16 depends from claim 1, and further recites:

> responsive to a determination that a target password has been retrieved:
> determining a change target password policy; and
> applying the change target password policy to modify the target password to match the second single sign-on password to create the modified target password.

A fundamental notion of patent law is the concept that invention lies in the new combination of old elements. Therefore, a rule that every invention could be rejected as obvious by merely locating each element of the invention in the prior art and combining the references to formulate an obviousness rejection is inconsistent with the very nature of "invention." Consequently, a rule exists that a combination of references made to establish a *prima facie* case of obviousness must be supported by some teaching, suggestion, or incentive contained in the prior art which would have led one of ordinary skill in the art to make the claimed invention.

The Examiner bears the burden of establishing a *prima facie* case of obviousness based on the prior art when rejecting claims under 35 U.S.C. § 103. *In re Fritch*, 972 F.2d 1260, 23 U.S.P.Q.2d 1780 (Fed. Cir. 1992). The requirements for establishing a *prima facie* case of obviousness in view of a combination of references are set forth in detail in Section 2142 of the MPEP and include the requirements that the Examiner explain in detail why the combination of the teachings is proper, that the Examiner provide a clear and convincing line of reasoning as to why an artisan would have found the claimed invention obvious in light of the teachings of the references, and that the Examiner provide a showing that it is the prior art and not the Applicant's own disclosure that teaches the combination asserted by the Examiner.

In rejecting claims 16, 35 and 54, the Examiner states:

> He disclosed retrieving and changing target passwords (See He Col. 13 Paragraphs 3-7), but He failed to disclose a change target password policy. However, He did disclose that having different administrative policies in individual network elements can be problematic (See He Col. 1 Paragraph 5).
>
> Prafullchandra teaches that requiring users to change passwords at predetermined intervals can enhance system security (See Prafullchandra Col. 2 Paragraph 3).
>
> It would have been obvious to the ordinary person skilled in the art at the time of the invention to employ the password aging and changing policy of Prafullchandra to the password changing system and method of He. This would have been obvious because the ordinary person skilled in the art would have been motivated to enhance the security in the network of He.

Final Office Action dated November 24, 2004, page 6.

Column 2, Paragraph 3 of Prafullchandra reads as follows:

> There are further difficulties with the present NIS+ password scheme, especially related to password aging. Password aging enhances system security by requiring a user to select a new password at predetermined intervals and preventing password updates before a certain period of time has elapsed. The current NIS+ configuration allows users

to access and alter their password aging information. Thus, password aging cannot be controlled by the system, which decreases the level of system security.

In the above recitation, Prafullchandra merely discusses the importance of changing passwords at predetermined intervals. Nowhere does Prafullchandra discuss that "in response to a determination that a target password has been retrieved", "determining a change target password policy", and "applying the change target password policy to modify the target password to match the second single sign-on password to create the modified target password" as recited in claim 16. Only the present application contains such disclosure. Claim 16 should, accordingly, be allowable in its own right as well as by virtue of its dependency from claim 1.

Claims 35 and 54 recite limitations similar to claim 16, and should also be allowable in their own right as well as by virtue of their dependency from claims 20 and 39, respectively.

Therefore, claims 16, 35 and 54 are believed to patentably distinguish over He in view of Prafullchandra, and it is respectfully requested that the Board reverse the Examiner's final rejection of those claims.

D. GROUND OF REJECTION 4 (Claims 17-19, 36-38, 55-57)

Claims 17-19, 36-38 and 55-57 stand rejected under 35 U.S.C. §103(a) as being unpatentable over He in view of Prafullchandra.

In rejecting the claims, the Examiner states that He discloses different types of passwords including standard user passwords, network element passwords, and super-user passwords. The Examiner then contends that it would have been obvious to one of ordinary skill in the art to employ the aging policy of Prafullachandra to all types of passwords of He because "the ordinary person skilled in the art would have been motivated to enhance the security of all the passwords, regardless of their type".

Claims 17-19, 36-38 and 55-57, however, depend from and further restrict dependent claims 16, 35 and 54, respectively, which in turn depend from and further restrict independent claims 1, 20 and 39. As described in detail above, Prafullchandra does not supply the deficiencies in He, and claims 17-19, 36-38 and 55-57 are not obvious over He in view of Prafullchandra.

Therefore, claims 17-19, 36-38 and 55-57 are believed to patentably distinguish over He in view of Prafullchandra, and it is respectfully requested that the Board so find and reverse the Examiner's final rejection of those claims.

James O. Skarsten
Reg. No. 28,346
Gerald H. Glanzman
Reg. No. 25,035
YEE & ASSOCIATES, P.C.
PO Box 802333
Dallas, TX 75380
(972) 385-8777

CLAIMS APPENDIX

The text of the claims involved in the appeal are:

1. A method in a data processing system for changing a plurality of target passwords in a single sign-on environment, comprising the steps of:

in response to receiving a change instruction identifying a first single sign-on password, changing the first single sign-on password to create a second single sign-on password;

retrieving a target password; and

modifying the target password in a user selected manner to match the second single sign-on password to create a modified target password.

2. The method as recited in claim 1, further comprising:

storing the modified target password;

responsive to a request from a user requesting access to an application, retrieving the modified target password; and

providing the changed target password to the requested application.

3. The method of claim 1, further comprising:

transmitting the modified target password to a client.

4. The method as recited in claim 2, wherein the requested application is located at a client.

5. The method of claim 1, wherein the user is prompted to modify the target password from a menu of possible target password modification methods.

6. The method in claim 5, wherein one of the possible target password modification methods is a common password source.

7. The method of claim 6, wherein the common password source is the second single sign-on password.

8. The method of claim 5, wherein one of the possible target password modification methods is a user supplied source.

9. The method of claim 5, wherein one of the possible target password modification methods is a random supplied source.

10. The method of claim 9, wherein the random supplied source is from a server.

11. The method of claim 9, further comprising:

determining a password policy; and

applying the password policy to generate random passwords.

12. The method of claim 11, wherein the password policy is a user level password policy.

13. The method of claim 11, wherein the password policy is an organizational level password policy.

14. The method of claim 11, wherein the password policy is a cell level password policy.

15. The method of claim 5, wherein the menu of possible target password modification methods is in a graphical user interface.

16. The method of claim 1, further comprising:

responsive to a determination that a target password has been retrieved:

determining a change target password policy; and

applying the change target password policy to modify the target password to match the second single sign-on password to create the modified target password.

17. The method of claim 16, wherein the change target password policy is applied at a user level.

18. The method of claim 16, wherein the change target password policy is applied at an organizational level.

19. The method of claim 16, wherein the change target password policy is applied at a cell level.

20. A computer program product in computer readable media for use in a data processing system for changing a plurality of target passwords in a single sign-on environment, the computer program product comprising:

first instructions for, in response to receiving a change instruction identifying a first single sign-on password, changing the first single sign-on password to create a second single sign-on password;

second instructions for retrieving a target password; and

third instructions for modifying the target password in a user selected manner to match the second single sign-on password to create a modified target password.

21. The computer program product of claim 20, further comprising:

fourth instructions storing the modified target password;

fifth instructions, responsive to a request from a user requesting access to an application, for retrieving the modified target password; and

sixth instructions, responsive to the fifth instructions, for providing the modified target password to the requested application.

22. The computer program product as recited in claim 20, further comprising:

fourth instructions for transmitting the modified target password to a client.

23. The computer program product as recited in claim 21, wherein the requested application is located at a client.

24. The computer program product as recited in claim 20, wherein the user is prompted to modify the target password from a menu of possible target password modification methods.

25. The computer program product as recited in claim 24, wherein one of the possible target password modification methods is a common password source.

26. The computer program product as recited in claim 25, wherein the common password source is the second single sign-on password.

27. The computer program product as recited in claim 24, wherein one of the possible target password modification methods is a user supplied source.

28. The computer program product as recited in claim 24, wherein one of the possible target password modification methods is a random supplied source.

29. The computer program product as recited in claim 28, wherein the random supplied source is from a server.

30. The computer program product as recited in claim 28, further comprising:

fourth instructions for determining a password policy; and

fifth instructions, responsive to the fourth instructions, for applying the password policy to generate random passwords.

31. The computer program product as recited in claim 30, wherein the password policy is a user level password policy.

32. The computer program product as recited in claim 30, wherein the password policy is an organizational password policy.

33. The computer program product as recited in claim 30, wherein the password policy cell level password policy.

34. The computer program product as recited in claim 24, wherein the menu of possible target password modification methods is in a graphical user interface.

35. The computer program product as recited in claim 20, further comprising:

fourth instructions for, responsive to a determination that a target password has been retrieved, determining a change target password policy; and

fifth instructions for, responsive to the fourth instructions, applying the change target password policy to modify the target password to match the second single sign-on password to create the modified target password.

36. The computer program product as recited in claim 35, wherein the change target password policy is applied at a user level.

37. The computer program product as recited in claim 35, wherein the change target password policy is applied at an organizational level.

38. The computer program product as recited in claim 35, wherein the change target password policy is applied at a cell level.

39. A system for changing a target password in a single sign-on environment, comprising:

in response to receiving a change instruction identifying a first single sign-on password, means for changing the first single sign-on password to create a second single sign-on password;

means for retrieving a target password; and

means for modifying the target password in a user selected manner to match the second single sign-on password to create a modified target password.

40. The system as recited in claim 39, further comprising:

means for storing the modified target password;

responsive to a request from a user requesting access to an application, means for retrieving the modified target password; and

means for providing the modified target password to the requested application.

41. The system as recited in claim 39, further comprising:

transmitting the modified target password to a client.

42. The system as recited in claim 40, wherein the requested application is located at a client.

43. The system as recited in claim 39, wherein the user is prompted to modify the target password from a menu of possible target password modification methods.

44. The system as recited in claim 43, wherein one of the possible target password modification methods is a common password source.

45. The system as recited in claim 44, wherein the common password source is the second single sign-on password.

46. The system as recited in claim 43, wherein one of the possible target password modification methods is a user supplied source.

47. The system as recited in claim 43, wherein one of the possible target password modification methods is a random supplied source.

48. The system as recited in claim 47, wherein the random supplied source is from a server.

49. The system as recited in claim 47, further comprising:

means for determining a password policy; and

means for applying the password policy to generate random passwords.

50. The system as recited in claim 49, wherein the password policy is a user level password policy.

51. The system as recited in claim 49, wherein the password policy is an organizational level password policy.

52. The system as recited in claim 49, wherein the password policy is a cell level password policy.

53. The system as recited in claim 43, wherein the menu of possible target password modification methods is in a graphical user interface.

54. The system as recited in claim 39, further comprising:

responsive to a determination that a target password has been retrieved, means for determining a change target password policy; and

responsive to the means for determining a change target password policy, means for applying the change target password policy to modify the target password to match the second single sign-on password to create the modified target password.

55. The system as recited in claim 54, wherein the change target password policy is applied at a user level.

56. The system as recited in claim 54, wherein the change target password policy is applied at an organizational level.

57. The system as recited in claim 54, wherein the change target password policy is applied at a cell level.

EVIDENCE APPENDIX

There is no evidence to be presented.

RELATED PROCEEDINGS APPENDIX

There are no related proceedings.